PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-187009
(43)Date of publication of application : 09.07.1999

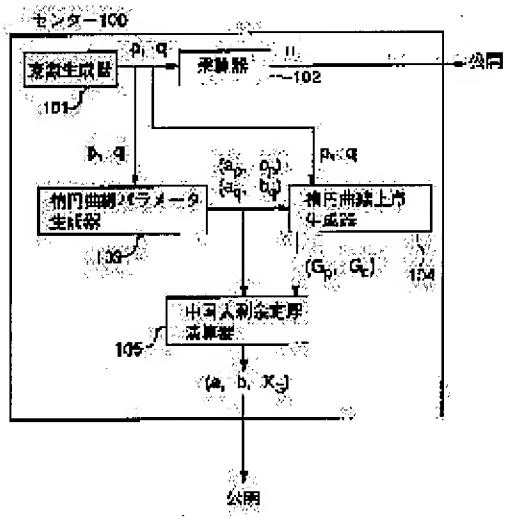
(51)Int.Cl. H04L 9/08
G09C 1/00
G09C 1/00

(21)Application number : 09-349167
(22)Date of filing : 18.12.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : OKAMOTO TATSUAKI
UCHIYAMA SHIGENORI

(54) NON-COMMUNICATION KEY DELIVERING METHOD, EQUIPMENT THEREFOR AND PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a non-communication key delivering system without a threshold value, of a simple algorithm and of good efficiency by utilizing a special elliptic curve on which the discrete logarithm is easily calculated.
SOLUTION: A center 100 can easily calculate the discrete logarithm of the elliptic curve En on n=pq (obtaining SA satisfying SA*G=h(IDA, rA) from G, h(IDA, rA) as it knows prime numbers (p) and (q). In addition, as SB generated similarly to SA, h(IDB, rB)=SB*G. Consequently, SA*h(IDB, rB)= SA*(SB*G)=(SASB)*G=SB*(SA*G)=SB*h(IDA, rA). Thus, a key KAB which a user A calculates from his secret key SA and the identifier IDB of a user B and a key KBA which the user B calculates from his secret key SB and the identifier IDA of the user A are coincident with each other.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－187009

(43)公開日　平成11年(1999)７月９日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｄ
Ｇ０９Ｃ	1/00	６２０	Ｇ０９Ｃ	1/00	６２０Ａ
					６２０Ｚ
		６３０			６３０Ｄ

審査請求　未請求　請求項の数14　ＯＬ　（全６頁）

(21)出願番号　特願平9－349167

(22)出願日　平成９年(1997)12月18日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　岡本　龍明
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　内山　成憲
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

(54)【発明の名称】　無交信鍵配送方法、その装置、及びプログラム記録媒体

(57)【要約】

【課題】　しきい値がなく、処理アルゴリズムが単純で効率が良い。

【解決手段】　センターＴで素数ｐ，ｑからｐ×ｑ＝ｎを作り、ｎを法とする環上での楕円曲線E_nのパラメータａ，ｂとE_n上の点の座標Ｇを作り、ａ，ｂ，Ｇ，ｎを公開し、ｐ，ｑを秘密に保持し、利用者ＡのID_Aと整数r_Aとより$X=h(ID_A, r_A)$を求め（１０６）、$X^3+aX+b \bmod n$が平方剰余となる最小のr_Aを求め（１０７）、そのＸを用いた$Y^2=X^3+aX+b \bmod n$点をＦ＝（Ｘ，Ｙ）とし、このＦに対し剰余演算を行い（１０８）、更に$s_A * G = F$を満すs_Aを求め（１０５）、s_AをＡの利用者鍵とし、ＡがＢと通信する際には、同様の条件を満すｈ（ID_B，r_B）を求め、$s_A * h(ID_B, r_B)$を共通暗号鍵とする。

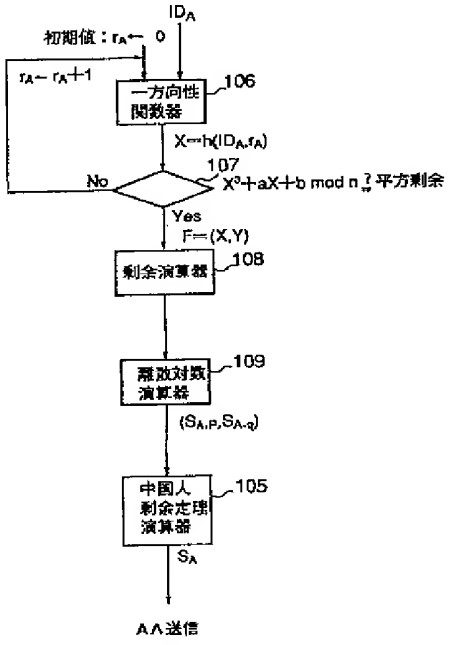


図３

1

【特許請求の範囲】

【請求項１】　鍵生成センター装置と多数の利用者Ａ，Ｂ，…，の利用者装置とからシステムが構成され、

システムの初期設定段階において、鍵生成センター装置は合成数ｎとｎを法とする剰余類環上での楕円曲線E_nのパラメータ及びE_n上の点Ｇをシステムの共通パラメータとし公開し、ｎの素因数を鍵生成センター装置に秘密鍵として秘密に保存し、

利用者鍵の生成段階において、鍵生成センター装置は、利用者Ａの識別子$I D_A$から関数Ｆを用いてＦ（$I D_A$）を計算し、上記秘密鍵を用いて、楕円曲線上の演算s_A＊Ｇ＝Ｆ（$I D_A$）を満足する利用者鍵s_Aを計算し、s_Aを利用者Ａの利用装置に秘密に配送し、

無交信鍵配送段階において、利用者Ａがその利用者装置と利用者Ｂの利用者装置とにより利用者Ｂと交信する際に、利用者Ａの利用者装置は利用者鍵s_Aと利用者Ｂの識別子$I D_B$からs_A＊Ｆ（$I D_B$）を計算し、利用者Ｂとの共通の暗号鍵K_{AB}とすることを特徴とする無交信鍵配送方法。

【請求項２】　上記利用者Ａの利用者鍵の生成は、識別子$I D_A$と整数r_Aとの連結を変数とする一方向性関数値Ｘが上記楕円曲線上の点のｘ座標となる最小の整数r_Aを求め、その条件を満す楕円曲線の点を剰余演算して上記Ｆ（$I D_A$）を求めることを特徴とする請求項１記載の無交信鍵配送方法。

【請求項３】　上記共通暗号鍵K_{AB}の生成において、上記識別子$I D_B$と整数r_Bとの連結を変数とする一方向性関数値が上記楕円曲線の点のｘ座標となる最小の整数r_Bを求めて上記Ｆ（$I D_B$）を得ることを特徴とする請求項１又は２記載の無交信鍵配送方法。

【請求項４】　自己の利用者鍵s_Aを保持する手段と、通信相手Ｂの識別情報$I D_B$と、公開されている楕円曲線E_nのパラメータとその曲線E_n上の公開されている点ＧとからＦ（$I D_B$）を計算する手段と、

上記Ｆ（$I D_B$）と上記利用者鍵s_Aとの上記楕円曲線E_n上での加算演算s_A＊Ｆ（$I D_B$）を計算して上記通信相手Ｂとの共通の暗号鍵K_{AB}を得る手段とを具備する無交信共通暗号鍵生成利用者装置。

【請求項５】　上記点Ｆ（$I D_B$）計算手段は、

上記識別情報$I D_B$と整数r_Bの連結を変数とする一方向性関数値を求める関数演算手段と、

上記求めた一方向性関数値を変数とし、上記楕円曲線のパラメータ、公開情報ｎを法とする値Ｚを求める剰余演算手段と、

上記値Ｚがｎを法とした平方剰余である最小の上記整数r_Bを求める手段と、

よりなることを特徴とする請求項４記載の無交信共通暗号鍵生成利用者装置。

【請求項６】　上記最小のr_Bを求める手段は、上記値Ｚが（Ｚ／ｎ）＝１であるか否かを検査するヤコビ記号演算手段と、

上記一方向性関数値をｘ座標とする点を上記楕円曲線上でｎ回加算すると無限遠点になるか否かを検査する楕円曲線上加算手段と、

上記ヤコビ記号演算手段の検査が１であり、かつ上記楕円曲線上加算手段の検査で加算値が無限遠点になることを満すまで上記整数r_BをＯより順次大とする手段と、よりなることを特徴とする請求項５記載の無交信共通暗号鍵生成利用者装置。

【請求項７】　無交信で共通暗号鍵を生成するために利用者装置で実行するプログラムを記録した記録媒体であって、

上記プログラムは、

通信相手Ｂの識別情報$I D_B$と、公開されている楕円曲線E_nのパラメータと、その曲線E_n上の点の座標とから、楕円曲線E_n上の点Ｆ（$I D_B$）を計算する過程と、

上記Ｆ（$I D_B$）と自己の秘密鍵s_Aとの楕円曲線E_n上での加算演算s_A＊Ｆ（$I D_B$）を行い共通暗号鍵K_{AB}を得る過程と、

を行うことを特徴とするコンピュータ読出し可能な記録媒体。

【請求項８】　上記点Ｆ（$I D_B$）を計算する過程は、上記識別情報$I D_B$と整数r_Bの連結を変数とする一方向性関数値を求める過程と、

公開情報ｎを法として、上記求めた一方向性関数値を変数とし、上記楕円曲線E_nの関数値Ｚを求める過程と、

上記値Ｚがｎを法とした平方剰余である最小の整数r_Bを求める過程とよりなることを特徴とする請求項７記載の記録媒体。

【請求項９】　上記最小のr_Bを求める過程は、

上記値Ｚが（Ｚ／ｎ）＝１か否かを検査するヤコビ記号演算過程と、

上記一方向性関数値を楕円曲線E_n上でｎ回加算する無限遠点になるかを検査する楕円曲線上加算過程と、

上記ヤコビ記号演算過程の検査が１であり、かつ上記楕円曲線上加算過程の検査で加算値が無限遠点になることを同時に満すまで上記整数r_BをＯから順次大とする過程とよりなることを特徴とする請求項８記載の記録媒体。

【請求項１０】　合成数ｎを生成し公開する手段と、ｎを法とする環上での楕円曲線E_nのパラメータ及びE_n上の点Ｇを生成して公開する手段と、

上記ｎの素因数を秘密鍵として秘密に保持する手段と、利用者Ａの識別子$I D_A$から関数Ｆを用いてＦ（$I D_A$）を計算する手段と、上記秘密鍵を用いて、楕円曲線E_n上の演算s_A＊Ｇ＝Ｆ（$I D_A$）を満足するs_Aを計算する手段と、

上記s_Aを上記利用者Ａの秘密鍵としてその利用者装置に秘密に配送する手段とを具備する無交信鍵配送センタ

一装置。

【請求項１１】　上記Ｆ（ＩＤA）を計算する手段は、上記ＩＤA と整数ｒA の連結を変数として一方向性関数値Ｘ＝ｈ（ＩＤA，ｒA）を求める手段と、

上記Ｘを変数として上記楕円曲線En に代入したものが平方剰余を満す最小の整数ｒA を求める手段と、

上記最小の整数ｒA にもとづく上記Ｘを上記楕円曲線Ｅn に代入しかつ法ｎの剰余演算を満す点を求めて上記Ｆ（ＩＤA）を得る手段とよりなることを特徴とする請求項１０記載の無交信鍵配送センター装置。

【請求項１２】　多数の利用者Ａ，Ｂ，…，に対し、利用者間で交信することなく鍵を配送する無交信鍵配送センター装置で実行するプログラムを記録した記録媒体であって、

上記プログラムは、

合成数ｎを生成し公開する過程と、

ｎを法とする環上での楕円曲線En のパラメータ及びEn 上の点Ｇを生成して公開する過程と、

上記ｎの素因数を秘密鍵として秘密に保持する過程と、

利用者Ａの識別子ＩＤA から関数Ｆを用いてＦ（ＩＤA）を計算する過程と、

上記秘密鍵を用いて楕円曲線En 上の演算sA ＊Ｇ＝Ｆ（ＩＤA）を満足するsA を計算する過程と、

上記sA を上記利用者Ａの利用者鍵としてその利用者装置へ秘密に配送する過程とを行うコンピュータ読出し可能な記録媒体。

【請求項１３】　上記Ｆ（ＩＤA）を計算する過程は、上記ＩＤA と整数ｒA の連結を変数として一方向性関数値Ｘ＝ｈ（ＩＤA，ｒA）を求める過程と、

上記Ｘを変数として上記楕円曲線En に代入した値が平方剰余を満す最小の整数ｒA を求める過程と、

上記最小の整数ｒA にもとづく上記Ｘを上記楕円曲線Ｅn に代入しかつ法ｎの剰余演算を満す点を求めて上記Ｆ（ＩＤA）を得る過程と、

を有することを特徴とする請求項１２記載の記録媒体。

【請求項１４】　上記ｎを生成する過程は、素数ｐ，ｑを生成する過程と、ｐとｑの積を求めて上記ｎとする過程とを有し、

上記パラメータ及び点Ｇを生成する過程は、上記ｐ及びｑに対し、それぞれ点の個数がｐ及びｑである楕円曲線Ep （ap，bp）及びEq （aq，bq）のパラメータ（ap，bp），（aq，bq）を生成する過程と、楕円曲線Ep，Eq 上の点のGp，Gq を求めて上記点Ｇを得る過程とよりなることを特徴とする請求項１２又は１３記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、電気通信システムにより暗号通信用の鍵を配送する鍵配送方法、特に利用者間で交信することなく鍵を配送する無交信鍵配送方法（岡本、山本著「現代暗号」産業図書）を実現する方法、その装置、及びそのプログラム記録媒体に関する。

【０００２】

【従来の技術】無交信鍵配送方式は、許容不正利用者数にしきい値がある方式としきい値が無い方式に大別される（岡本、山本著「現代暗号」産業図書、13.5.2節）。しきい値がある方式の代表例は、松本、今井によるＫＰＳ（Matsumoto，T. and Imai，H. ：On the Key Predistribution System ：A Practical Solution to the Key Distribution Problem，Proc. of Crypto'87，ＬＮＣＳ 293，Springer-Verlag，pp.185-193(1988)）であるが、しきい値があるため、一定数以上の利用者がそれぞれの秘密鍵を持ち寄ると、それからシステム共通の秘密鍵が計算でき、システム全体が崩壊する。

【０００３】しきい値が無い方式の代表例は、辻井らによるＮＩＫＳ－ＴＡＳ（Tsujii，S.，Araki，K.，Kasahara，M.，Okamoto，E.，Sakai，R.，Maeda，Y.，and Yagisawa，T. ：On Ambiguity in Coppersmith' Attacking Methodagainst ＮＩＫＳ－ＴＡＳ Scheme，ＩＥＩＣＥ Trans. Fundamentals，E79-A，1，pp.66-75(1996)）である。しかし、この方式は処理アルゴリズムが大変複雑で、単に効率性に問題があるのみならず、安全性の検証が困難である。

【０００４】

【発明が解決しようとする課題】この発明の目的は、しきい値が無く、処理アルゴリズムが単純で効率の良い無交信鍵配送システム及びそのプログラム記録媒体を提供することにある。

【０００５】

【課題を解決するための手段】ある特殊な楕円曲線では、その上での離散対数が容易に計算できるが、この発明では、そのような楕円曲線を利用することにより、無交信鍵配送方式を効率的に実現する。

【０００６】

【発明の実施の形態】図１に、この発明のシステム構成例を示す。鍵生成センターの装置（以降、センターと呼ぶ）１００と、利用者の装置（以降、利用者と呼ぶ）２００の複数とがそれぞれ通信回線等を介して接続している。

（１）システムの初期設定

図２を用いて、システムの初期設定処理の説明を行う。センター１００は、素数生成器１０１を用いて素数ｐ，ｑを生成し、乗算器１０２を用いて、ｎ＝ｐｑを計算し、さらに、ｐ，ｑを楕円曲線パラメータ生成器１０３に入力してパラメータ（ap，bp），（aq，bq）を出力する。ここで、生成された楕円曲線Ep （ap，bp）Eq （aq，bq）はそれぞれ、点の個数がｐおよびｑとなっている。このような楕円曲線のパラメータ生成の具体的なアルゴリズムは文献（Miyaji，A. ：Elliptic Curves over Fp Suitable for Cryptosystem

s, Proc. of Auscrypt'92, ＬＮＣＳ, Springer-Verlag , pp.479-504(1993)) に示されている。また、（a_p , b_p ），（a_q , b_q ）を楕円曲線上点生成器１０４に入力し、（G_p , G_q ）を出力する。（p, q）、（a_p , b_p ），（a_q , b_q ）及び（G_p , G_q ）を中国人剰余定理演算器１０５に入力し、（a, b）及びＧのｘ一座標、X_G を出力する。ここで、$a \equiv a_p \pmod p$，$a \equiv a_q \pmod q$，$b \equiv b_p \pmod p$，$b \equiv b_q \pmod q$，$G \equiv G_p \pmod p$，$G \equiv G_q \pmod q$ であり、以降これらを$a = [a_p, a_q]$ などと表記する。

【０００７】センター１００は、p，qを秘密鍵として保持し、（n，a，b，X_G ）を公開鍵として公開する。

（２）利用者鍵の生成

図３を用いて、利用者鍵の生成処理の説明を行う。センター１００は、以下の手順で、利用者Ａ２００の識別子$I D_A$ からＡの秘密鍵s_A を生成する。

【０００８】まず、Ａは、$r_A = 0$に対して、ハッシュ関数のような一方向性関数の関数演算器１０６を用いて、$X = h(I D_A, r_A)$ を計算し、さらに平方剰余判定器１０７を用いて$X^3 + aX + b \bmod n$が平方剰余かどうか判定し、平方剰余ならば、つまりＸが楕円曲線Ｅ上の点のｘ座標となったので、そのY² ≡X³ ＋ａＸ＋ｂ（mod ｎ）を満足する点をＦ＝（Ｘ，Ｙ）とし、剰余演算器１０８を用いて、$F_p = F \bmod p$ and $F_q = F \bmod q$をそれぞれ演算する。もし、判定器１０７で平方剰余でないと判定すると、r_A の値を１だけ増やし、同様の手続きを繰り返し行い、平方剰余となる最小のr_A を見つける。

【０００９】次に、センター１００は、離散対数演算器１０９を用いて、

$s_{A,p}\ G_p = F_p$, $s_{A,q}\ G_q = F_q$

を満す$s_{A,p}$, $s_{A,q}$ を計算する。ここで、このアルゴリズムは文献（Satoh , T. , and Araki , K. : Fermat Quotient and the Polynomial Time DiscreteLog Algorithm for Anomalous Elliptic Curves, Preprint (September , 1997) 、to appear in the Proceedings of ＰＫＣ'98 , ＬＮＣＳ, Springer-Verlag)に示されている。さらに、中国剰余定理演算器１０５を用いて$s_A = [s_{A,p}, s_{A,q}]$ を計算する。

【００１０】センター１００は、（s_A , r_A ）を利用者Ａ２００に秘密に送信する。

（３）無交信鍵配送

図４を用いて、無交信鍵配送処理の説明を行う。利用者Ａ２００は、以下の手順で、利用者Ｂとの間の暗号鍵K_{AB} をＢと交信することなく生成する。まず、利用者Ａは、以下の検査を行いこれらを同時に満足する最小のr_B （$r_B \geq 0$）を求める。

・関数演算器２０６及び剰余演算器２０１を用いてＺ＝$h(I D_B, r_B)^3 + a\,h(I D_B, r_B) + b \bmod n$を計算し、さらにヤコビ記号演算器２０２を用いて（Ｚ／ｎ）＝１となるかどうかを検査する。ヤコビ記号の計算アルゴリズムは文献（Knuth , D. E. , : The Art of Computer Programming , Addison-Wesley Publishing Co. , (1981)）等に記されている。（Ｚ／ｎ）＝１ということは２分の１の確率で、上記Ｚの式がｎを法とする平方剰余であることになる。

・楕円曲線のｘ一座標加算演算器２０３を用いて$n * h(I D_B, r_B) = \infty$となるかどうかを検査する。なお、ｎ＊Ｘは、楕円曲線E_n のある点のｘ一座標であるＸに対してｘ一座標加算演算をｎ回適用したものを意味する。この楕円曲線のｘ一座標加算演算の計算式は、文献（Demytko , N. : A New Elliptic Curve Based Analogue of ＲＳＡ, Proc. of Eurocrypt'93 , ＬＮＣＳ 765, Springer-Verlag , pp.40-49(1994)）に示されている。つまり$n * h(I D_B, r_B) = \infty$とは楕円曲線$E_n$ 上の点$h(I D_B, r_B)$ をｎ回加算演算した結果は無限遠点になる（この楕円曲線E_n の位数はｎ）ことを意味する。

【００１１】次に、ｘ一座標加算演算器２０３を用いて、利用者Ａ２００は、

$K_{AB} = s_A * h(I D_B, r_B)$

を計算する。

【００１２】

【発明の効果】この発明では、センター１００は素数p，qを知っているためｎ＝ｐｑ上での楕円曲線E_n の離散対数（G，$h(I D_A, r_A)$ より、$s_A * G = h(I D_A, r_A)$ を満足するs_A を求めること）が容易に計算できる。更にs_B もs_A と同様に作られたものであるから$h(I D_B, r_B) = s_B * G$であり、従って$s_A * h(I D_B, r_B) = s_A * (s_B * G) = (s_A s_B) * G = s_B * (s_A * G) = s_B * h(I D_A, r_A)$ が成立するため、利用者Ａが自分の秘密鍵s_A と利用者Ｂの識別子$I D_B$ より計算した鍵K_{AB} と、利用者Ｂが自分の秘密鍵s_B と利用者Ａの識別子$I D_A$ より計算した鍵K_{BA} が一致する。つまり、利用者ＡとＢは無交信で鍵を共有することが可能となる。

【００１３】システムの初期設定における、センターで必要とされる処理は十分に効率的に実現が可能であり、パーソナルコンピュータで数分程度の時間で生成できる。詳しくは、文献（Miyaji, A. : Elliptic Curves over F_p Suitable for Cryptosystems, Proc. of Auscrypt'92, ＬＮＣＳ, Springer-Verlag , pp.479-504(1993)）を参照されたい。

【００１４】利用者鍵の生成における、センターで必要とされる処理も十分に効率的に実現が可能であり、一人の利用者の鍵生成に要する処理量は、鍵サイズの３乗のオーダーである（つまり、ＲＳＡ暗号の復号程度の処理量である）。各利用者の無交信鍵配送に要する処理量も

鍵サイズの３乗のオーダーである。上記に示すように、この発明によれば、単純な原理に基づいており、その安全性の解析は比較的容易である。つまり、この発明の安全性は、楕円曲線E_nが与えられて、（Ｘ，ｓ＊Ｘ，ｔ＊Ｘ）から（ｓｔ）＊Ｘを求める問題の難しさと同等である。

【図面の簡単な説明】

【図１】この発明方法が適用されるシステムの構成例を

示すブロック図。

【図２】センター装置におけるシステム初期設定時に行う処理に必要な機能構成例を示す図。

【図３】センター装置における利用者鍵の生成に必要な機能構成例を示す図。

【図４】利用者装置で無交信共通暗号鍵の生成に必要な機能構成例を示す図。

【図１】

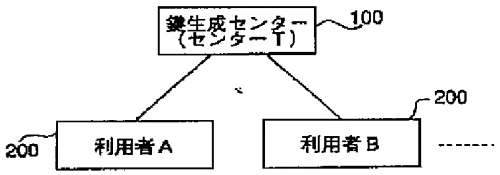


図 1

【図２】

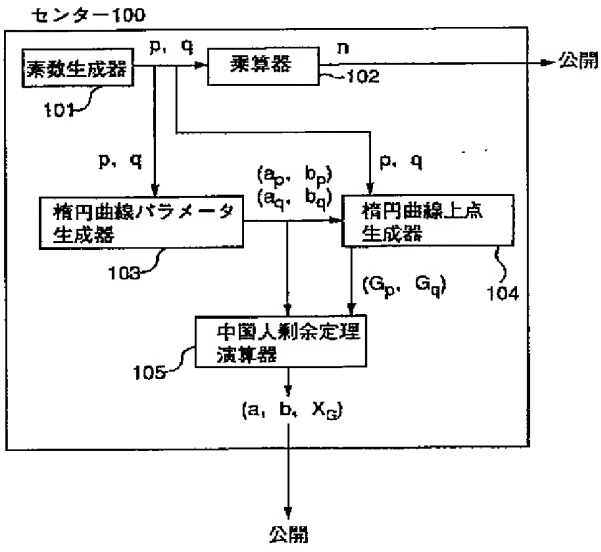


図 2

【図３】

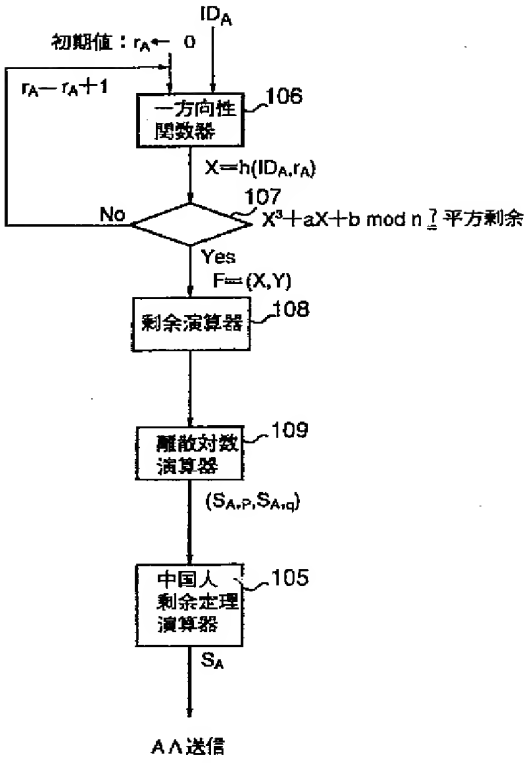

ID_A
初期値：r_A← 0
r_A—r_A+1
一方向性関数器
106
X=h(ID_A,r_A)
No
107
X^3+aX+b mod n ? 平方剰余
Yes
F=(X,Y)
剰余演算器
108
離散対数演算器
109
($S_{A,P}$,$S_{A,q}$)
中国人剰余定理演算器
105
S_A
AA送信

図 3

【図４】

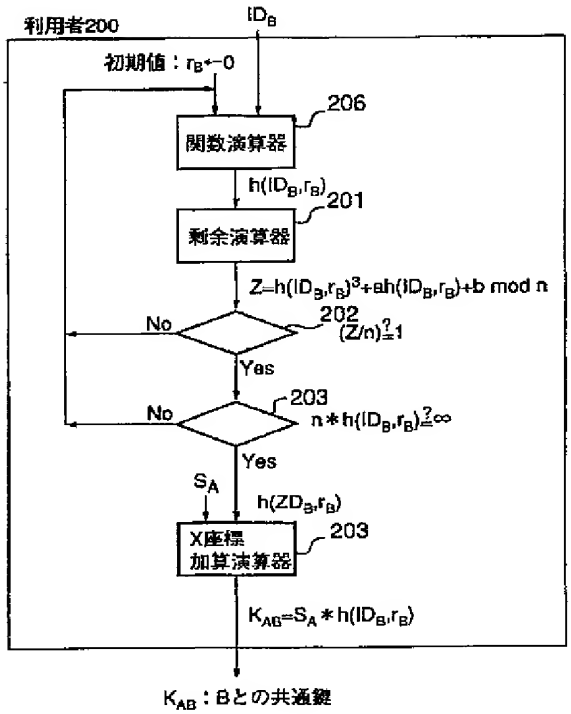

利用者200
ID_B
初期値：r_B←0
関数演算器
206
h(ID_B,r_B)
剰余演算器
201
Z=h(ID_B,r_B)^3+ah(ID_B,r_B)+b mod n
No
202
(Z/n)?=1
Yes
No
203
n*h(ID_B,r_B)?=∞
Yes
S_A
h(ZD_B,r_B)
X座標加算演算器
203
K_{AB}=S_A*h(ID_B,r_B)
K_{AB}：Bとの共通鍵

図 4